Image: ©Wavebreakmedia Ltd/thinkstockphotos

FAQ – Penetration Testing and IT Security Analysis

You would like to learn more about penetration testing and IT security analysis? We have answered the most important questions below.

1. WHAT IS A PENETRATION TEST AND AN IT SECURITY ANALYSIS?

During a penetration test and an IT security analysis we simulate a realistic cyberattack on your IT infrastructure from a hacker's perspective. This allows our experts to identify existing or potential vulnerabilities in your IT before attackers can exploit them.

2. WHAT ARE THE ADVANTAGES OF PENETRATION TESTING AND THE IT SECURITY CONCEPT?

You receive a comprehensive overview of the vulnerabilities in your network, IT system, applications and mobile devices. Our experts show you how to protect yourself permanently from network attacks to prevent industrial espionage and harmful unauthorized access. This allows you to protect the confidentiality and integrity of your data and reduce your liability risk.

3. WHAT IS THE PROCEDURE FOR CREATING AN IT SECURITY CONCEPT?

We collect all the information relevant for an attack and examine your company from the perspective of an attacker. Once we have identified vulnerabilities we attempt to access them in the role of an external or internal attacker. Then we document and analyze the identified weak points and work with you to develop relevant countermeasures.

www.tuv.com/en/pentest

TÜVRheinland®
Precisely Right.

4. WHAT AREAS ARE COVERED BY THE IT SECURITY ANALYSIS MODULES?

- Infrastructures
- Mobile applications
- WLAN
- Central components
- Web applications
- Rich/fat clients and other applications
- Source code analysis
- IT-Forensic
- Embedded Devices

5. DO I NEED TO PROTECT MYSELF FROM NETWORK ATTACKS EVEN AS A SMALL BUSINESS?

Yes, because no company is too small for an attack. We have applied our experience successfully even for small businesses and in a variety of industries.

6. WOULD I DETECT A NETWORK ATTACK?

No, not necessarily. Many businesses have already fallen victim to criminal hackers without noticing.

7. IS A ONE-OFF SECURITY CHECK ENOUGH?

A security check is always a snapshot. Both the attacks and the tested infrastructure or application continue to develop, so that test results become less valuable over time. Therefore such tests should be conducted regularly. They do not have to cover all aspects, but can instead focus on any changes.

YOU HAVE A DIFFERENT QUESTION? CONTACT OUR EXPERTS NOW, WE ARE HAPPY TO HELP.

ONLINE CONTACT

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806 – 0
service@i-sec.tuv.com
www.tuv.com/en/pentest

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval.